Available at: http://www.ictp.trieste.it/~pub_off IC/98/57

United Nations Educational Scientific and Cultural Organization
and
International Atomic Energy Agency

THE ABDUS SALAM INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

TAME KERNELS AND TATE KERNELS OF QUADRATIC NUMBER FIELDS

Qin Hourong*
Department of Mathematics, Nanjing University,
Nanjing 210093, People's Republic of China
and
The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

Abstract

Let F be a quadratic field. We obtain the necessary and sufficient conditions for an element of order two in the tame kernel of F to be a fourth power in the tame kernel of F. This enables us to compute the 8-rank of the tame kernel of F. In the case when F is an imaginary quadratic field with the 8-rank of $K_2O_F = 0$, the explicit structure of the Tate kernel of F can be obtained by our method.

MIRAMARE – TRIESTE
June 1998

* E-mail: hrqin@ictp.trieste.it

1. Introduction

Let $F = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ square-free, be a quadratic field, O_F the ring of integers of F. We know that any element of order 2 in K_2O_F can be written as the form $\{-1, x\}$, where x has been given explicitly by A.Schinzel and J. Browkin [1]. Therefore, we can determine the 2^n-rank of K_2O_F if we can give the necessary and sufficient conditions for $\{-1, x\} = \alpha^{2^{n-1}}$ with $\alpha \in K_2O_F$. We have done this for $n = 2$ in [16] and [17]. The purpose of this paper is to consider the same problem for the case $n = 3$. The paper is organized as follows.

Section 2 contains a review of known material, some of which is stated in the form needed here.

In section 3, we study the fourth power problem in K_2O_F, some results are valid for the K_2 group of a general field. We present the main theorem of the paper, which gives the necessary and sufficient conditions for an element $\{-1, x\} \in K_2O_F$ being a fourth power in K_2O_F, where F is a quadratic field.

Finally, in sections 4 and 5, we apply the results in section 3 to the imaginary quadratic fields and the real quadratic fields respectively. The 8-rank of K_2O_F has been determined for any quadratic field whose discriminant has only one odd prime divisor. At the same time the Tate kernel of F is given if F is an imaginary quadratic field with the 8-rank of $K_2O_F = 0$.

2. Preliminaries

In this section, we will introduce some notations, recall some known facts, and give some immediate corollaries to known results.

We begin with the following lemma, which is very useful in this paper.

Lemma 2.1(Legendre's Theorem). *Suppose that a, b, c are square-free, $(a, b) = (a, c) = (b, c) = 1$ and a, b, c do not have the same sign. Then the Diophantine equation*

$$aX^2 + bY^2 + cZ^2 = 0 \tag{2.1}$$

has nontrivial solutions if and only if for every odd prime $p \mid abc$, say, $p \mid a$, $\left(\frac{-bc}{p}\right) = 1$.

Proof. See [11].

We have also

Lemma 2.2(Holzer's Theorem). *If (2.1) is solvable, then it has a nontrivial integer solution with*

$$|X| \leq \sqrt{|bc|}, \qquad |Y| \leq \sqrt{|ca|}, \qquad |Z| \leq \sqrt{|ab|}$$

Proof. See [11].

Corollary 2.3. *Suppose that the Diophantine equation $X^2 + dY^2 + mZ^2 = 0$ has a nontrivial solution and $w \in \mathbb{N}$ with $(w, m) = 1$. Then it has a solution $X_1, Y_1, Z_1 \in \mathbb{Z}$ satisfying $(Z_1, w) \stackrel{2}{=} 1$. Here $(Z_1, w) \stackrel{2}{=} 1$ means that (Z_1, w) has no any odd prime divisor.*

Proof. Let $X_0, Y_0, Z_0 \in \mathbb{Z}$ with $(X_0, Y_0, Z_0) = 1$ be a solution of $X^2 + dY^2 + mZ^2 = 0$. Then for any $x \in \mathbb{Z}$, one can verify that

$$\begin{cases} X = X_0(x^2 + m) - 2x(X_0x + mZ_0) \\ Y = Y_0(x^2 + m) \\ Z = Z_0(x^2 + m) - 2(X_0x + mZ_0) \end{cases}$$

is also a solution. (See [11] for the result on the form of the general solutions of $aX^2 + bY^2 + cZ^2 = 0$.) For any odd prime p, if $p \mid (Z_0, w)$, set $x \equiv 1 \pmod{p}$; if $p \mid w, p \nmid Z_0$, then

$$Z_0(x^2 + m) - 2(X_0x + mZ_0) \equiv Z_0(x + s)^2 + t \pmod{p},$$

where $s, t \in \mathbb{Z}$. Choose $r \not\equiv 0 \pmod{p}$ such that $Z_0(x + s)^2 + t \equiv r \pmod{p}$ is solvable. Then by the Chinese Remainder Theorem, there are $X_1, Y_1, Z_1 \in \mathbb{Z}$ with $(Z_1, w) \stackrel{2}{=} 1$ satisfying $X_1^2 + dY_1^2 + mZ_1^2 = 0$. This completes the proof.

Remark 2.3.1. In view of Lemma 2.2 and the above proof, we see that Z_1 can be chosen depending only on (Z_0, w) and d.

From now on, when we say a (quadratic) Diophantine equation is solvable, we always mean that it has nontrivial solutions.

Let $d \neq 0$ be an integer. It is convenient for us to use the following notation:

$$S(d) = \begin{cases} \{\pm 1, \pm 2\}, & \text{if } d > 0, \\ \{1, 2\}, & \text{if } d < 0. \end{cases}$$

For any abelian group A, let A_2 denote the 2-Sylow subgroup of A, and let ${}_2A = \{x \in A \mid x^2 = 1\}$. Let F be a number field, O_F the ring of integers of F, denote by Ω the set of all places of F. For any $\wp \in \Omega$ and $a, b \in F_\wp$, $\left(\frac{a,b}{\wp}\right)$ is the Hilbert symbol with order 2 on $F_\wp$. In particular, on $\mathbb{Q}_2$, we have

$$\left(\frac{u,v}{2}\right) = (-1)^{\frac{(u-1)(v-1)}{4}} \quad \text{and} \quad \left(\frac{2,u}{2}\right) = (-1)^{\frac{u^2-1}{8}},$$

where u, v are units in $\mathbb{Q}_2$. For more about the Hilbert symbols, we refer to [12] or [13]. For any finite place $\wp$ of F, we use $v_\wp(\cdot)$ to denote the discrete valuation on F with respect to $\wp$ and $\tau_\wp$ for the tame symbol at $\wp$. For any integer n, put $\bigtriangledown^n = \{\alpha \in K_2O_F \mid \alpha = \beta^n \text{ for some } \beta \in K_2O_F\}$.

Lemma 2.4 [1]. *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free. Then ${}_2K_2O_F$ can be generated by*

$$\{-1, m\}, \qquad m \mid d;$$

together with

$$\{-1, u_i + \sqrt{d}\},$$

if $\{-1, \pm 2\} \bigcap NF \neq \emptyset$, where $u_i \in \mathbb{Z}$ such that $u_i^2 - d = c_i w_i^2$ for some $w_i \in \mathbb{Z}$ and $c_i \in \{-1, \pm 2\} \bigcap NF$.

Lemma 2.5 [16],[17]. *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free. Suppose that $m \mid d$ and write $d = u^2 - 2w^2$ with $u, w \in \mathbb{Z}$ if $2 \in NF$. Then $\{-1, m\} \in \bigtriangledown^2$ if and only if one can find an $\epsilon \in S(d)$ such that*

(i) $\left(\frac{\frac{d}{m}}{p}\right) = \left(\frac{-\epsilon}{p}\right)$, *for any odd prime $p \mid m$;*

(ii) $\left(\frac{m}{p}\right) = \left(\frac{\epsilon}{p}\right)$, *for any odd prime $p \mid \frac{d}{m}$;*

and $\{-1, m(u + \sqrt{d})\} \in \bigtriangledown^2$ if and only if

(iii) $\left(\frac{\frac{d}{m}}{p}\right) = \left(\frac{-\epsilon(u+w)}{p}\right)$, *for any odd prime $p \mid m$;*

(iv) $\left(\frac{m}{p}\right) = \left(\frac{\epsilon(u+w)}{p}\right)$, *for any odd prime $p \mid \frac{d}{m}$.*

For a real quadratic number field F, we have the following map

$$K_2O_F \longrightarrow \mu_2 \oplus \mu_2.$$

It is clear that for any $\alpha \in K_2O_F$, if $\alpha = \beta^2$ with $\beta \in K_2F$, then the image of α is $(1,1)$. One can see that if there are $m \in \mathbb{N}$ and $\epsilon < 0$ such that both (i) and (ii) in Lemma 2.5 are satisfied, then the image of α is either $(-1, 1)$ or $(1, -1)$, where $\alpha \in K_2O_F$ with $\alpha^2 = \{-1, g\}$. Hence, if $-1, -2 \notin NF$, then $\{-1, m\} \notin \bigtriangledown^4$. This fact has been used to determine the structure of $(K_2O_F)_2$ for some real quadratic fields in [15]. On the other hand, if -1 or $-2 \in NF$ and there are $m \in \mathbb{N}$ and $\epsilon < 0$ such that both (i) and (ii) are satisfied, then one can show that both (i) and (ii) are also valid for the same m and $-\epsilon$. Therefore, we have

Lemma 2.6. *Let $F = \mathbb{Q}(\sqrt{d})$ be a quadratic field and $\alpha \in {}_2K_2O_F$. If $\alpha \in \nabla^4$, then there is an $\epsilon \in \{1, 2\}$ such that*
$\epsilon m z^2 = x^2 + dy^2$ is solvable if $\alpha = \{-1, m\}$,
or
$\epsilon m(u + w)z^2 = x^2 + dy^2$ is solvable if $\alpha = \{-1, m(u + \sqrt{d})\}$.

Lemma 2.7 [16],[17]. *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free, be a quadratic field. For any $\alpha = x + y\sqrt{d} \in F$, put $S = \{\wp_1, ..., \wp_n\} = \{\wp, |\tau_\wp\{-1, \alpha\} = -1\}$. Without loss of generality, we can assume that $p_i = \wp_i \cap \mathbb{Z}$ is not inert for $1 \leq i \leq n$. Then $x^2 - dy^2 = \epsilon p_1 \cdots p_n z^2$, where $\epsilon \in S(d)$ and $z \in \mathbb{Q}$. Conversely, suppose that $p_1, ..., p_n$ are distinct primes in $\mathbb{Z}$ and $\wp_1, ..., \wp_n$ are prime ideals of O_F such that $\wp_i \cap \mathbb{Z} = p_i$ for $1 \leq i \leq n$. If there is an $\epsilon \in S(d)$ such that the equation $x^2 + dy^2 = \epsilon p_1 \cdots p_n z^2$ is solvable in $\mathbb{Q}$ (equivalently in $\mathbb{Z}$), then there is an $\alpha \in F^*$ such that $S = \{\wp | \tau_\wp\{-1, \alpha\} = -1\} = \{\wp_1, ..., \wp_n\}$.*

Lemma 2.8 [14]. *Let F be a field, $\gamma \in K_2F$ with $\gamma^4 = 1$. Then there are $x, y \in F^*$, such that $\gamma = \{x, x^2 + 1\}\{-1, y\}$.*

3. Fourth powers in K_2O_F

Although we will focus on quadratic fields, we first give some results on symbols in the general case.

Lemma 3.1. *Let F be a field. Suppose that $x, y, c \in F^*$ with $x + y = c^n$. Then*

$$\{x, y\} = \left\{-\frac{x}{y}, c\right\}^n.$$

Proof. $\{x, y\} = \{x, c^n - x\} = \left\{x, c^n(1 - \frac{x}{c^n})\right\} = \{x, c^n\}\left\{x, 1 - \frac{x}{c^n}\right\} =$
$\{x, c^n\}\left\{\frac{x}{c^n}, 1 - \frac{x}{c^n}\right\}\left\{c^n, 1 - \frac{x}{c^n}\right\} = \{x, c\}^n\{c, y\}^n\{c^n, c^n\} = \left\{-\frac{x}{y}, c\right\}^n.$
This completes the proof.

The identities in the following lemma will be used repeatedly.

Lemma 3.2. *Let F be a field. If $a \in F^*$ and $a = x^2 + y^2$ with $x, y, x - y \in F^*$. Then*

$$\{-1, a\} = \left\{\frac{2xy}{x^2 + y^2}, \frac{x - y}{x}\right\}^4 \{2, x\}^4\{x^2 + y^2, 2\}^2.$$

If $a = s^2 \pm 2t^2$ with $s, t \in F^*$, then

$$\{\mp 2, a\} = \{2t^2, s\}^2\left\{\frac{s}{r}, a\right\}^2.$$

Proof. $\{-1, a\} = \{-1, x^2 + y^2\} = \left\{\frac{y}{x}, \frac{x^2 + y^2}{x^2}\right\}^2$
$= \left\{-\frac{2y}{x}, \frac{x^2 + y^2}{x^2}\right\}^2\left\{-\frac{1}{2}, \frac{x^2 + y^2}{x^2}\right\}^2.$
By Lemma 3.1, $\left\{-\frac{2y}{x}, \frac{x^2 + y^2}{x^2}\right\} = \left\{\frac{2xy}{x^2 + y^2}, \frac{x - y}{x}\right\}^2$. Hence,
$\{-1, a\} = \left\{\frac{2xy}{x^2 + y^2}, \frac{x - y}{x}\right\}^4 \{2, x\}^4\{x^2 + y^2, 2\}^2.$
Now suppose that $a = s^2 + 2t^2$. Then
$\{-2, a\} = \{-2, s^2 + 2t^2\} = \{-2t^2, s^2 + 2t^2\}\left\{\frac{1}{t^2}, s^2 + 2t^2\right\}.$
By Lemma 3.1, $\{-2t^2, s^2 + 2t^2\} = \left\{\frac{2t^2}{s^2 + 2t^2}, s\right\}^2$, hence,
$\{-2, a\} = \{2t^2, s\}^2\{\frac{s}{r}, s^2 + 2t^2\}^2.$

Similarly, we can verify that $\{2, a\} = \{2t^2, s\}^2\left\{\frac{s}{r}, s^2 - 2t^2\right\}^2$ if $a = s^2 - 2t^2$. The proof is complete.

Corollary 3.3. *Let F be a field, and let $a \in F^*$. If $a = x^2 + y^2 = (c^2 - 2d^2)(e^2 + 2f^2)$ (especially, $c^2 - 2d^2$ or $e^2 + 2f^2$) for some $x, y, c, d, e, f \in F^*$, then there is an element $\gamma \in K_2F$ with $\gamma^4 = \{-1, a\}$. In particular, if $-1 = x^2 + y^2$, then $\{-1, -1\} = \gamma^4$ holds for some $\gamma \in K_2F$, in other words, $\{-1, -1\} = \alpha^2$ if and only if $\{-1, -1\} = \beta^4$, where $\alpha, \beta \in K_2K$.*

Proof. The result is just a consequence of Lemmas 3.1 and 3.2.

Lemma 3.4. *Let $F = \mathbb{Q}(\sqrt{d})$ be a quadratic field.*

(i) Suppose $m \mid d$. Assume that $m > 0$ if $d > 0$ and $m \equiv 1 \pmod 4$ if $d \equiv 1 \pmod 8$. Then there is a prime $p \equiv 1 \pmod 4$ such that

$$\epsilon pmZ^2 = X^2 + dY^2$$

is solvable for $\epsilon = 1$ or 2.

(ii) Suppose $2 \in NF, d = u^2 - 2w^2$, where $u, w \in \mathbb{Z}$ and $m \mid d$. Assume that $mu > 0$ if $d > 0$ and $m(u + w) \equiv 1 \pmod 4$ if $d \equiv 1 \pmod 8$. Then there is a prime $p \equiv 1 \pmod 4$ such that

$$\epsilon pm(u + w)Z^2 = X^2 + dY^2$$

is solvable for $\epsilon = 1$ or 2.

Proof. (i). We may rewrite the equation

$$\epsilon pmZ^2 = X^2 + dY^2$$

as

$$\epsilon pZ^2 = mX^2 + \frac{d}{m}Y^2 \tag{3.1}$$

By Lemma 2.1, (3.1) is solvable if and only if there is a prime $p \equiv 1 \pmod 4$ such that

$$\begin{aligned} \left(\frac{d}{p}\right) &= 1, \\ \left(\frac{\frac{d}{m}}{l}\right) &= \left(\frac{\epsilon p}{l}\right), \text{ for any odd prime } l \mid m, \\ \left(\frac{m}{l}\right) &= \left(\frac{\epsilon p}{l}\right), \text{ for any odd prime } l \mid \frac{d}{m}. \end{aligned}$$

If $2 \mid d$, then we choose $p \equiv 1 \pmod 4$ such that both $\left(\frac{\frac{d}{2}}{p}\right) = \pm 1$ and $\left(\frac{d}{p}\right) = 1$ hold.

If $d > 0$ is odd, then we want to find a prime $p \equiv 1 \pmod p$ such that both $\left(\frac{\frac{d}{m}}{m}\right)\left(\frac{m}{\frac{d}{m}}\right) = \left(\frac{\epsilon p}{d}\right)$ and $\left(\frac{d}{p}\right) = 1$ hold for some $\epsilon = 1$ or 2.

Suppose that $m \equiv 1 \pmod 4$ or $\frac{d}{m} \equiv 1 \pmod 4$, then we can take $\epsilon = 1$.

Suppose that $d \equiv 5 \pmod 8$ and $m \equiv 3 \pmod 4$, then we can take $\epsilon = 2$.

Suppose that $d \equiv 1 \pmod 8$, then we must have $m \equiv 1 \pmod 4$, hence, we can take $\epsilon = 1$.

If $d < 0$ is odd, then we require

$$\left(\frac{\frac{d}{m}}{|m|}\right)\left(\frac{m}{|\frac{d}{m}|}\right) = \left(\frac{\epsilon p}{|d|}\right). \tag{3.2}$$

Suppose that $|d| \equiv 3$ or $5 \pmod 8$, then it is easy to see that there is a prime $p \equiv 1 \pmod 4$ such that both $\left(\frac{d}{p}\right) = 1$ and (3.2) hold for an $\epsilon = 1$ or 2.

Suppose that $|d| \equiv 1 \pmod 8$, one can verify that

$$\left(\frac{\frac{d}{m}}{|m|}\right)\left(\frac{m}{|\frac{d}{m}|}\right) = 1.$$

Suppose that $|d| \equiv 7 \pmod 8$, then the only possibility is that $m \equiv 1 \pmod 4$. Hence, by the assumption, we have

$$\left(\frac{\frac{d}{m}}{|m|}\right)\left(\frac{m}{|\frac{d}{m}|}\right) = 1.$$

Therefore, in both cases, taking $\epsilon = 1$, we see that there is a prime $p \equiv 1 \pmod 4$ such that both $\left(\frac{d}{p}\right) = 1$ and (3.2) hold.

The proof of (ii) is similar, so we complete the proof.

Lemma 3.5. *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free. Suppose that prime $p \mid d$. Then there is a $\gamma \in K_2F$ such that*

(i) $\{2, p\} = \gamma^2$ *with* $\tau_\wp \gamma = \begin{cases} 2 & \text{if } \wp \mid p, \\ 1 & \text{otherwise} \end{cases}$ *if* $p \equiv 1, 7 \pmod 8$;

(ii) $\{-2, p\} = \gamma^2$ *with* $\tau_\wp \gamma = \begin{cases} -2 & \text{if } \wp \mid p, \\ 1 & \text{otherwise} \end{cases}$ *if* $p \equiv 3 \pmod 8$.

Proof. If $p \equiv 1$ or $7 \pmod 8$, then $p = a^2 - 2b^2$ with $a, b \in \mathbb{Z}$. By Lemma 3.2, we have

$$\{2, p\} = \{2b^2, a\}^2 \left\{\frac{a}{b}, p\right\}^2.$$

Put $\gamma = \{2b^2, a\}\left\{\frac{a}{b}, p\right\}$. Then it is easy to see that γ has the desired property.

In the case where $p \equiv 3 \pmod 8, p = a^2 + 2b^2$ with $a, b \in \mathbb{Z}$. We have

$$\{-2, p\} = \{2b^2, a\}^2 \left\{\frac{a}{b}, p\right\}^2.$$

Taking $\gamma = \{2b^2, a\}\left\{\frac{a}{b}, p\right\}$ yields the result. The lemma is proved.

Lemma 3.6. *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free. Suppose that $p \mid d$ and $p \equiv 5 \pmod 8$ is a prime. Then there is a prime q with $\left(\frac{d}{q}\right) = 1$ such that*

(i) $pqZ^2 = X^2 + 2dY^2$ is solvable if d is even or $d \equiv 3 \pmod 8$;

(ii) $2pqZ^2 = X^2 + 2dY^2$ is solvable if $d \equiv 5$ or $7 \pmod 8$.

Moreover, in each case, there is a $\gamma \in K_2F$ with

$$\tau_\wp \gamma = \begin{cases} 2, & \text{if } \wp \mid p, \\ -1, & \text{if } \wp = \mathfrak{q}_1, \\ 1, & \text{if } \wp = \mathfrak{q}_2, \text{ where } \mathfrak{q}_1\mathfrak{q}_2 = qO_F, \\ 1, & \text{otherwise} \end{cases}$$

such that $\gamma^2 = \{2, p\}$.

Proof. (i). Suppose d is even. Let $d = 2d'$. Rewrite

$$pqZ^2 = X^2 + 2dY^2$$

as

$$qZ^2 = pX^2 + \frac{2d'}{p}Y^2 \tag{3.3}$$

By Lemma 2.1, we require that there is a prime q with $\left(\frac{d'}{q}\right) = 1$ and $\left(\frac{q}{|d'|}\right) = 1$ if we want (3.3) to be solvable. Hence we may choose $q \equiv 1 \pmod 8$, so $\left(\frac{d}{q}\right) = 1$.

Now let $X_0, Y_0, Z_0 \in \mathbb{Z}$ with $(X_0, Y_0) = (X_0, Z_0) = (Y_0, Z_0) = 1$ be a solution of (3.3). It follows from $\left(\frac{d}{q}\right) = 1$ that $\left(\frac{-2}{q}\right) = 1$. Hence, $q = a^2 + 2b^2$ for some $a, b \in \mathbb{Z}$.

Since $X_0^2 + 2dY_0^2 = X_0^2 + 2(\sqrt{d}Y_0)^2$, by Lemma 3.2,

$\{-2, X_0^2 + 2dY_0^2\} = \{2dY_0^2, X_0\}^2 \left\{\frac{X_0}{\sqrt{d}Y_0}, X_0^2 + 2dY_0^2\right\}^2$ and

$\{a^2 + 2b^2, -2\} = \{a, 2b^2\}^2 \left\{q, \frac{a}{b}\right\}^2$.

Therefore, $\{-2, p\} = \{-2, pqZ_0^2\}\{qZ_0^2, -2\}$

$= \{-2, X_0^2 + 2dY_0^2\}\{q, -2\}\{Z_0, -2\}^2$

$= \{2dY_0^2, X_0\}^2 \left\{\frac{X_0}{\sqrt{d}Y_0}, X_0^2 + 2dY_0^2\right\}^2 \{a, 2b^2\}^2 \left\{q, \frac{a}{b}\right\}^2 \{Z_0, -2\}^2$.

Put

$$\gamma = \{2dY_0^2, X_0\} \left\{\frac{X_0}{\sqrt{d}Y_0}, X_0^2 + 2dY_0^2\right\} \{a, 2b^2\} \left\{q, \frac{a}{b}\right\} \{Z_0, -2\}.$$

Since $\left(\frac{d}{q}\right) = 1$, we have $qO_F = \mathfrak{q}_1\mathfrak{q}_2$, where $\mathfrak{q}_1, \mathfrak{q}_2$ are the prime ideals of O_F.

Clearly, for $i = 1, 2$, $\tau_{\mathfrak{q}_i}\{2dY_0^2, X_0^2\} = \tau_{\mathfrak{q}_i}\{2b^2, a\} = 1$. We may assume further that for $i = 1, 2$, $\tau_{\mathfrak{q}_i}\{Z_0, 2\} = 1$.

On the other hand, for $i = 1, 2$,

$$\tau_{\mathfrak{q}_i}\left\{\frac{X_0}{\sqrt{d}Y_0}, X_0^2 + 2dY_0^2\right\} \equiv \frac{X_0}{\sqrt{d}Y_0} \pmod{\mathfrak{q}_i}$$

and

$$\tau_{\mathfrak{q}_i}\left\{q, \frac{b}{a}\right\} \equiv \frac{b}{a} \pmod{\mathfrak{q}_i}.$$

We have $\tau_{\mathfrak{q}_i}\gamma^2 \equiv 1 \pmod{\mathfrak{q}_i}$, since $\left(\frac{X_0}{\sqrt{d}Y_0}\frac{b}{a}\right)^2 = \frac{X_0^2 b^2}{dY_0^2 a^2} \equiv 1 \pmod q$.

Note that it is impossible that both

$$\tau_{\mathfrak{q}_1}\gamma \equiv c \pmod{\mathfrak{q}_1}$$

and

$$\tau_{\mathfrak{q}_2}\gamma \equiv c \pmod{\mathfrak{q}_2}$$

hold at the same time, where $c = 1$ or -1. In fact, if it is the case, then

$$\frac{X_0}{\sqrt{d}Y_0}\frac{b}{a} \equiv c \pmod{\mathfrak{q}_i} \text{ for } i = 1, 2,$$

hence, $\frac{X_0}{\sqrt{d}Y_0}\frac{b}{a} \equiv c \pmod q$, therefore, $X_0 b - ca\sqrt{d}Y_0 \equiv 0 \pmod q$, this is a contradiction since $(q, X_0 b) = 1$.

A computation shows that

$$\tau_\wp\gamma \equiv 2 \pmod{\wp}, \text{for } \wp \mid p$$

and

$$\tau_\wp\gamma \equiv 1 \pmod{\wp}, \text{for any } \wp \nmid pq.$$

The similar discussion works for the other cases and our lemma is proved.

One can use the same method to show the following

Lemma 3.7. *Let $F=\mathbb{Q}(\sqrt{d}), d\in\mathbb{Z}$ square-free, and let $d\equiv 1 \pmod 8$. Suppose that $m\mid d$ with $m>0$.*

(i) If $m\equiv 1 \pmod 8$, then we can find a prime q with $\left(\frac{d}{q}\right)=1$ such that $qmZ^2=X^2-2dY^2$ is solvable. Furthermore, there is a $\gamma\in K_2F$ with

$$\tau_\wp\gamma=\begin{cases}2, & \text{if } \wp\mid m;\\ -1, & \text{if } \wp=\mathfrak{q}_1;\\ 1, & \text{if } \wp=\mathfrak{q}_2(\mathfrak{q}_1\mathfrak{q}_2=qO_F);\\ 1, & \text{otherwise}\end{cases}$$

such that $\{2,m\}=\gamma^2$.

(ii) If $d<0$ and $m\equiv 5 \pmod 8$, then we can find a prime q with $\left(\frac{d}{q}\right)=1$ such that $-2qmZ^2=X^2-2dY^2$ is solvable. Furthermore, there is a $\gamma\in K_2F$ with

$$\tau_\wp\gamma=\begin{cases}2, & \text{if } \wp\mid m;\\ -1, & \text{if } \wp=\mathfrak{q}_1;\\ 1, & \text{if } \wp=\mathfrak{q}_2(\mathfrak{q}_1\mathfrak{q}_2=qO_F);\\ 1, & \text{otherwise}\end{cases}$$

such that $\{2,m\}=\gamma^2$.

(iii) If $d>0$ and $m\equiv 5 \pmod 8$, then we can find a prime q with $q\equiv 3 \pmod 8$ such that $qmZ^2=X^2-2dY^2$ is solvable. Furthermore, there is a $\gamma\in K_2F$ with

$$\tau_\wp\gamma=\begin{cases}2, & \text{if } \wp\mid m;\\ i(i^2\equiv -1 \pmod{\wp}), & \text{if } \wp=qO_F;\\ 1, & \text{otherwise}\end{cases}$$

such that $\{2,m\}\{-1,q\}=\gamma^2$.

Lemma 3.8. *Let $d\in\mathbb{Z}$ square-free. Suppose that there are $u,w\in\mathbb{Z}$ such that $d=u^2-2w^2$. Then there is a prime $q\equiv 1$ or $3 \pmod 8$ such that*

$$X^2+2dY^2=uqZ^2 \tag{3.4}$$

is solvable if one of the following conditions is satisfied

(i) $d\not\equiv 1 \pmod 8$ or $d<0$;

(ii) $d\equiv 1 \pmod 8$ together with $d>0$ and $\left(\frac{u}{d}\right)=1$.

For the case where $d\equiv 1 \pmod 8), d>0$ and $\left(\frac{u}{d}\right)=-1$, there is a prime $q\equiv 7 \pmod 8$ such that

$$X^2+2dY^2=uqZ^2 \tag{3.5}$$

is solvable.

Proof. This is proved by explicit calculations of Jacobi symbols. We will not go into details.

Remark 3.8.1. If $d\equiv 1 \pmod 8, d<0$ and $\left(\frac{u}{|d|}\right)=-1$, then $\left(\frac{-u}{|d|}\right)=1$.

With the same notations as above, suppose that $X^2+2dY^2=uqZ^2$ is solvable and $X_0,Y_0,Z_0\in\mathbb{N}$ a solution. Put

$$n=Y_0,\qquad m=\frac{X_0-2wY_0}{u}.$$

By the choice of X_0,Y_0 and Z_0, we can assume that $n,m\in\mathbb{Z}$ with $(n,m)=1$. Let

$$g=m^2-2n^2,\qquad e=m^2+2n^2$$

and

$$x = -2wng + mqZ_0^2, \qquad y = me,$$
$$a = 2wmg + 2nqZ_0^2, \qquad b = 2ne.$$

Then

$$(a + b\sqrt{d})^2 + 2(x + y\sqrt{d})^2 = (u + \sqrt{d})(2eZ_0)^2.$$

In fact, we have

$$eu + 4wmn = qZ_0^2 \quad \text{and} \quad g^2 - e^2 = -8m^2n^2.$$

Hence, $a^2 + b^2d + 2(x^2 + y^2d)$
$= a^2 + 2x^2 + (b^2 + 2y^2)d$
$= (2wmg + 2nqZ_0^2)^2 + 2(-2wng + mqZ_0^2)^2 + (4n^2e^2 + 2m^2e^2)(u^2 - 2w^2)$
$= 4w^2m^2g^2 + 4n^2q^2Z_0^4 + 8w^2n^2g^2 + 2m^2q^2Z_0^4 + 2e^3(u^2 - 2w^2)$
$= 4w^2g^2e + 2q^2Z_0^4e + 2e^3(u^2 - 2w^2)$
$= 2e(q^2Z_0^4 + e^2u^2) + 4ew^2(g^2 - e^2)$
$= 2e(q^2Z_0^4 + e^2u^2) - 32ew^2m^2n^2$
$= 2e(q^2Z_0^4 + qZ_0^2(eu - 4wmn))$
$= 2eqZ_0^2(qZ_0^2 + eu - 4wmn)$
$= qu(2eZ_0)^2$
and

$$4xy + 2ab = 4m^2qeZ_0^2 + 8n^2qeZ_0^2 = q(2eZ_0)^2.$$

Write

$$H = x + y\sqrt{d}, \qquad G = a + b\sqrt{d}.$$

The above computation shows

$$G^2 + 2H^2 = q(u + \sqrt{d})(2eZ_0)^2.$$

By Lemma 3.2,

$$\{2, q(u + \sqrt{d})(2eZ_0)^2\} = \{2, G^2 + 2H^2\} = \{2H^2, G\}^2 \left\{\frac{G}{H}, G^2 + 2H^2\right\}^2.$$

If $q \equiv 1$ or $3 \pmod 8$, then there are $r, s \in \mathbb{Z}$ such that $q = r^2 + 2s^2$. Hence,

$$\{q, 2\} = \{r, 2s^2\}^2 \left\{q, \frac{r}{s}\right\}^2.$$

So, we get

$$\begin{aligned}\{2, u + \sqrt{d}\} &= \{2, q(u + \sqrt{d})(2eZ_0)^2\}\{q, 2\}\{(2eZ_0)^2, 2\} \\ &= \{2H^2, G\}^2 \left\{\frac{G}{H}, G^2 + 2H^2\right\}^2 \{r, 2s^2\}^2 \left\{q, \frac{r}{s}\right\}^2 \{2eZ_0, 2\}^2.\end{aligned}$$

Similarly, if $q \equiv 7 \pmod 8$, then $q = r^2 - 2s^2$ with $r, s \in \mathbb{Z}$. In this case,

$$\{q, -2\} = \{r, 2s^2\}^2 \left\{q, \frac{r}{s}\right\}^2.$$

Hence,

$$\{2, u + \sqrt{d}\}\{-1, q\} = \{2H^2, G\}^2 \left\{\frac{G}{H}, G^2 + 2H^2\right\}^2 \{r, 2s^2\}^2 \left\{q, \frac{r}{s}\right\}^2 \{2eZ_0, 2\}^2.$$

Put

$$\gamma = \{2H^2, G\} \left\{\frac{G}{H}, G^2 + 2H^2\right\} \{r, 2s^2\} \left\{q, \frac{r}{s}\right\} \{2eZ_0, 2\}.$$

Lemma 3.9. *Let everything be the same as above. Then by the choice of solutions of (3.4) or (3.5), we can assume that for any non-dyadic finite place* $\wp$,

$$\tau_\wp\gamma = \begin{cases} -1, & \text{if } \wp = \mathfrak{q}_1; \\ 1, & \text{if } \wp = \mathfrak{q}_2 (\mathfrak{q}_1\mathfrak{q}_2 = qO_F); \\ 2^{\frac{1}{2}v_\wp(u+\sqrt{d})}, & \text{if } \wp \mid (u+\sqrt{d}); \\ 1, & \text{otherwise} \end{cases}$$

if $d \not\equiv 1 \pmod 8$ *or* $d < 0$ *or* $d \equiv 1 \pmod 8$ *together with* $d > 0$, $\left(\frac{u}{d}\right) = 1$; *and*

$$\tau_\wp\gamma = \begin{cases} i, & (i^2 \equiv -1 \pmod \wp)), \text{ if } \wp = qO_F; \\ 2^{\frac{1}{2}v_\wp(u+\sqrt{d})}, & \text{if } \wp \mid (u+\sqrt{d}); \\ 1, & \text{otherwise.} \end{cases}$$

if $d \equiv 1 \pmod 8$ *together with* $d > 0$, $\left(\frac{u}{d}\right) = -1$.

Proof. It follows from $(m, n) = 1$ that $(e, m) = (e, n) = 1$, since $e = m^2 + 2n^2$. We can assume that $(q, w) = 1$, by Lemma 2.2, $(Z_0, w) \stackrel{2}{=} 1$, hence, $(e, w) = 1$ and $(e, q) = 1$. Clearly, we can assume that $(n, u) = 1$, so $(n, Z_0) = 1$.

We have
$$e = m^2 + 2n^2 \equiv \frac{X_0^2}{u^2} + 2Y_0^2 \equiv \frac{1}{u^2}(X_0^2 + 2dY_0^2) \equiv \frac{qZ_0^2}{u} \pmod w.$$

Hence,

$$\begin{aligned} x + y\sqrt{d} &\equiv mqZ_0^2 + me\sqrt{d} \pmod w \\ &\equiv m(qZ_0^2 + \frac{qZ_0^2}{u}\sqrt{d}) \pmod w \\ &\equiv \frac{mqZ_0^2}{u}(u+\sqrt{d}) \pmod w. \end{aligned}$$

Hence, for any non-dyadic finite place $\wp \mid (u+\sqrt{d}), v_\wp(x+y\sqrt{d}) \geq \frac{1}{2}v_\wp(u+\sqrt{d})$. Similarly, $v_\wp(a+b\sqrt{d}) \geq \frac{1}{2}v_\wp(u+\sqrt{d})$. Let $\mathbf{g} = v_\wp(G) = v_\wp(a+b\sqrt{d})$ and $\mathbf{h} = v_\wp(H) = v_\wp(x+y\sqrt{d})$. Then $\min(\mathbf{g}, \mathbf{h}) = \frac{1}{2}v_\wp(u+\sqrt{d})$, since $G^2 + 2H^2 = q(u+\sqrt{d})(2eZ_0)^2$, $(e, w) \stackrel{2}{=} 1$ and $Z_0, w) \stackrel{2}{=} 1$. Therefore, if $\mathbf{g} \geq \mathbf{h}$, then

$$\begin{aligned} \tau_\wp\gamma &\equiv \frac{(2H^2)^{\mathbf{g}}}{G^{2\mathbf{h}}} \cdot \frac{\left(\frac{G}{H}\right)^{2\mathbf{h}}}{(G^2+2H^2)^{\mathbf{g}-\mathbf{h}}} \pmod \wp \\ &\equiv 2^{\mathbf{g}} \cdot \left(\frac{H^2}{G^2+2H^2}\right)^{\mathbf{g}-\mathbf{h}} \pmod \wp \\ &\equiv 2^{\mathbf{h}} \pmod \wp \\ &\equiv 2^{\frac{1}{2}v_\wp(u+\sqrt{d})} \pmod \wp. \end{aligned}$$

A computation shows that $\tau_\wp\gamma \equiv 2^{\frac{1}{2}v_\wp(u+\sqrt{d})} \pmod \wp$ holds also for $\mathbf{g} \leq \mathbf{h}$.

One can verify that
$$mx + my\sqrt{d} + na + nb\sqrt{d} = e^2\sqrt{d}.$$

Therefore we have $v_\wp(G) = v_\wp(H) = 0$ for any $\wp \mid qZ_0$.

On the other hand, for any prime $l \mid e$,

$$x + y\sqrt{d} \equiv x \not\equiv 0 \pmod l \text{ and } a + b\sqrt{d} \equiv a \not\equiv 0 \pmod l.$$

It is easy to see that

$$\tau_\wp \gamma = 1 \text{ if } \wp \nmid q(u+\sqrt{d}).$$

Now suppose $\wp \mid q$.

If $\left(\dfrac{d}{q}\right) = 1$, then $qO_F = \mathfrak{q}\bar{\mathfrak{q}}$. We have

$$\tau_{\mathfrak{q}}\gamma \equiv \frac{G}{H}\cdot\frac{s}{r} \pmod{\mathfrak{q}}, \quad \tau_{\bar{\mathfrak{q}}}\gamma \equiv \frac{G}{H}\cdot\frac{s}{r} \pmod{\bar{\mathfrak{q}}}.$$

For $\wp = \mathfrak{q}$ or $\bar{\mathfrak{q}}$, since $\dfrac{G^2}{H^2}\cdot\dfrac{s^2}{t^2} \equiv 1 \pmod{\wp}$, we see that

$$\frac{G}{H}\cdot\frac{s}{r} \equiv \pm 1 \pmod{\wp}.$$

We claim that if $\dfrac{G}{H}\cdot\dfrac{s}{r} \equiv c \pmod{\mathfrak{q}}$, then $\dfrac{G}{H}\cdot\dfrac{s}{r} \equiv -c \pmod{\bar{\mathfrak{q}}}$, where $c = \pm 1$.

In fact, if both $\dfrac{G}{H}\cdot\dfrac{s}{r} \equiv c \pmod{\mathfrak{q}}$ and $\dfrac{G}{H}\cdot\dfrac{s}{r} \equiv c \pmod{\bar{\mathfrak{q}}}$ hold, then

$$\frac{G}{H}\cdot\frac{s}{r} \equiv c \pmod{q}, \text{ hence, } \frac{2wmg+2ne\sqrt{d}}{-2wng+me\sqrt{d}}\cdot\frac{s}{r} \equiv c \pmod{q}.$$

It follows that

$$-2cwngr \equiv 2wmgs \pmod{q}, \qquad cmer \equiv 2nes \pmod{q}.$$

This is the same as to say that

$$-cnr \equiv ms \pmod{q}, \qquad cmr \equiv 2ns \pmod{q}.$$

Hence, we have $m^2+2n^2 \equiv 0 \pmod{q}$. This is impossible since $e = m^2+2n^2$ and $(e,q)=1$. So, we can assume that $\tau_{\mathfrak{q}_1}\gamma = -1$ and $\tau_{\mathfrak{q}_2}\gamma = 1$, where $\mathfrak{q}_1\mathfrak{q}_2 = qO_F$.

If $q \equiv 7 \pmod 8$, then $\left(\dfrac{d}{q}\right) = -1$. Hence, qO_F is a prime ideal of O_F. In this case, $\dfrac{G^2}{H^2} \equiv -2 \pmod{qO_F}$ and $\dfrac{s^2}{r^2} \equiv \dfrac{1}{2} \pmod{qO_F}$. So, if we write $i = \dfrac{G}{H}\cdot\dfrac{s}{r}$, then $\tau_{qO_F}\gamma \equiv i \pmod{qO_F}$ with $i^2 \equiv -1 \pmod{qO_F}$. The lemma is proved.

In view of Lemma 2.5, we assume that $d \in \mathbb{Z}$ square-free, $m \mid d$ and $\epsilon m Z^2 = X^2 + dY^2$ is solvable for $\epsilon \in \{1,2\}$. Let $X_0, Y_0, Z_0 \in \mathbb{Z}$ with $(X_0, Y_0) = 1$ be a solution. Put

$$\rho = \left\{\frac{2X_0Y_0\sqrt{d}}{\epsilon m Z_0^2}, \frac{X_0 - Y_0\sqrt{d}}{X_0}\right\}\{2, X_0\}\{Z_0, -2\}.$$

By Lemma 3.2, $\rho^4\{m,2\}^2 = \{-1, m\}$. We need to compute the tame symbol of ρ.

Lemma 3.10. *With the same notations and assumptions, we can assume*

$$\tau_\wp \rho = \begin{cases} \left(\dfrac{Y_0\sqrt{d}}{X_0}\right)^{v_\wp(Z_0)} \pmod{\wp}, & \text{if } \wp \mid Z_0; \\ 2 \pmod{\wp}, & \text{if } \wp \mid m; \\ 1, & \text{otherwise.} \end{cases}$$

Proof. $\epsilon m Z_0^2 = X_0^2 + dY_0^2$ and $m \mid d$ imply that $m \mid X_0$, let $X_0 = mX_0'$. We can assume that $(d, Z_0) = 1$, hence, $(m, Y_0) = 1$. If $\wp \mid m$, then $v_\wp(X_0) \equiv 0 \pmod 2$, and

$$\begin{aligned}
\tau_\wp \rho &\equiv (-1)^{(-1+v_\wp(X_0))(1-v_\wp(X_0))} \cdot \frac{\left(\dfrac{2X_0Y_0\sqrt{d}}{\epsilon m Z_0^2}\right)^{1-v_\wp(X_0)}}{\left(\dfrac{X_0 - Y_0\sqrt{d}}{X_0}\right)^{-1+v_\wp(X_0)}} \cdot 2^{v_\wp(X_0)} \pmod \wp \\
&\equiv -1 \cdot \left(\frac{\epsilon m Z_0^2}{2(X_0 - Y_0\sqrt{d})Y_0\sqrt{d}}\right)^{v_\wp(X_0)-1} \cdot 2^{v_\wp(X_0)} \pmod \wp \\
&\equiv -1 \cdot \left(\frac{\epsilon Z_0^2}{2(X_0'\sqrt{d} - \dfrac{d}{m}Y_0)Y_0}\right)^{v_\wp(X_0)-1} \cdot 2^{v_\wp(X_0)} \pmod \wp \\
&\equiv -1 \cdot \left(\frac{\epsilon Z_0^2}{-2\dfrac{d}{m}Y_0^2}\right)^{v_\wp(X_0)-1} \cdot 2^{v_\wp(X_0)} \pmod \wp \\
&\equiv 2 \pmod \wp.
\end{aligned}$$

We have used the fact that $\epsilon Z_0^2 = mX_0' + \dfrac{d}{m}Y_0^2$.

For $\wp \mid Z_0$,

$$\begin{aligned}
\tau_\wp \rho &\equiv \left(\frac{X_0 - Y_0\sqrt{d}}{X_0}\right)^{2v_\wp(Z_0)} \cdot \left(-\frac{1}{2}\right)^{v_\wp(Z_0)} \pmod \wp \\
&\equiv \left(\frac{X_0^2 + dY_0^2 - 2X_0Y_0\sqrt{d}}{-2X_0^2}\right)^{v_\wp(Z_0)} \pmod \wp \\
&\equiv \left(\frac{Y_0\sqrt{d}}{X_0}\right)^{v_\wp(Z_0)} \pmod \wp.
\end{aligned}$$

If $\wp \mid \dfrac{d}{m}$, then $v_\wp\left(\dfrac{X_0 - Y_0\sqrt{d}}{X_0}\right) = 0$, hence, $\tau_\wp \rho = 1$.

If $\wp \nmid d$, $\wp \nmid Z_0$, then it is easy to see that $\tau_\wp \rho = 1$. This completes the proof.

Now we are going to deal with the case when $2 \in NF$. In this case, $d = u^2 - 2w^2$, $u, w \in \mathbb{Z}$ and for any odd prime divisor p of d, $p \equiv \pm 1 \pmod 8$.

Suppose that $m \mid d$ and $\epsilon m(u+w)Z^2 = X^2 + dY^2$ is solvable, where $\epsilon = 1$ or 2. Let $X_0, Y_0, Z_0 \in \mathbb{Z}$ be a nontrivial solution. Put

$$h = Y_0, \qquad g = \frac{X_0 - wY_0}{u + w}.$$

By the choice of X_0, Y_0 and Z_0, we can assume that $g, h \in \mathbb{Z}$ with $(g, h) = 1$. As in [16] and [17], write

$$\alpha = g^2 + h^2, \quad \theta = (g^2 - h^2 + 2gh)w, \quad \lambda = (g^2 - h^2 - 2gh)w.$$

We have the following identities

$$\alpha u + \theta = mZ^2, \qquad \lambda^2 + \theta^2 = 2\alpha^2 w^2.$$

Let

$$x = mZ_0^2(g+h) + \lambda(g-h), \qquad y = \alpha(g+h);$$

$$a = mZ_0^2(g-h) + \lambda(g+h), \qquad b = \alpha(g-h).$$

Then

$$\begin{aligned}
&x^2+a^2+(y^2+b^2)d\\
&= m^2Z_0^4(g+h)^2+\lambda^2(g-h)^2+m^2Z_0^4(g-h)^2+\lambda^2(g+h)^2\\
&\quad +\alpha^2(g+h)^2d+\alpha^2(g-h)^2d\\
&= 2m^2Z_0^4\alpha+2\lambda^2\alpha+2\alpha^3(u^2-2w^2)\\
&= 2\alpha(m^2Z_0^4+\lambda^2+2\alpha^2u^2-2\alpha^2w^2)\\
&= 2\alpha(m^2Z_0^4-\theta^2+\alpha^2u^2)\\
&= 2\alpha(\alpha u+\theta)(2\alpha u)\\
&= mu(2\alpha Z_0)^2.
\end{aligned}$$

And

$$2(xy+ab)+4mZ_0^2\alpha^2=m(2\alpha Z_0)^2.$$

Let

$$E=x+y\sqrt{d},\qquad F=a+b\sqrt{d}.$$

Then

$$E^2+F^2=m(u+\sqrt{d})(2\alpha Z_0)^2.$$

Put

$$\psi=\left\{\frac{2EF}{E^2+F^2},\frac{F-E}{F}\right\}\{2,F\}\{\alpha Z_0,-2\}.$$

Then

$$\psi^4\{m(u+\sqrt{d}),2\}^2=\{-1,(u+\sqrt{d})m\}.$$

Continuing to use the notations as above, we have

Lemma 3.11. *By a suitable choice of X_0,Y_0,Z_0, a solution of the Diophantine equation*

$$\epsilon(u+w)mZ_0^2=X_0^2+dY_0^2,$$

we can assume that

$$\tau_\wp\psi=\begin{cases}\left(\dfrac{E}{F}\right)^{v_\wp(Z_0)}, & \text{if } \wp\mid Z_0,\\ 2^{\frac{1}{2}v_\wp(u+\sqrt{d})}, & \text{if } \wp\mid(u+\sqrt{d});\\ 2, & \text{if } \wp\mid m;\\ 1, & \text{otherwise.}\end{cases}$$

Proof. We can take $\epsilon=1$, since $2\in NF$. Rewrite $m(u+w)Z^2=X^2+dY^2$ in the form $(u+w)Z^2=mX'^2+\dfrac{d}{m}Y^2$, where $X'=\dfrac{1}{m}X$. Applying Corollary 2.3, we can assume that $(dw,Z_0)\overset{2}{=}1$. The assumption $(g,h)=1$ implies that $(\alpha,Z_0)\overset{2}{=}1$. In fact, if there is an odd prime $l\mid(\alpha,Z_0)$, then $l\mid\theta$, since $\alpha u+\theta=mZ_0^2$. But $l\nmid w$, so we must have $l\mid(g^2-h^2-2gh)$. On the other hand, $g^2-h^2-2gh=\alpha-2h(g+h)$. Hence, $l\mid 2h(g+h)$, therefore, $l\mid h$ or $l\mid(g+h)$. If $l\mid h$, then $l\mid g$, contradicting the assumption $(g,h)=1$. If $l\mid(g+h)$, then we would have $l\mid g-h$, since $(g+h)^2+(g-h)^2=2\alpha^2$. Then $l\mid(g,h)$, is also a contradiction. The above discussion also shows that $(\alpha,w)\overset{2}{=}1$. The identity $x^2+a^2+(y^2+b^2)d=m(2\alpha Z_0)^2$ implies that $m\mid\lambda$. So we can assume that for any $\wp\mid m$,

$$\min(v_\wp(E),v_\wp(F))=v_\wp(F-E)=1.$$

Hence, in any case, for any $\wp\mid m$, we can show

$$\tau_\wp\psi=2.$$

Note that $x^2 - y^2 d \equiv a^2 - b^2 d \pmod{w}$ and $E^2 + F^2 = m(u+\sqrt{d})(2\alpha Z_0)^2$. Hence, we obtain that for any $\wp \mid (u+\sqrt{d})$,

$$\min(v_\wp(E), v_\wp(F)) = \frac{1}{2} v_\wp(u+\sqrt{d}).$$

Moreover, we can assume that $v_\wp(F-E) = \frac{1}{2} v_\wp(u+\sqrt{d})$. Hence, we can show that if $\wp \mid (u+\sqrt{d})$, then

$$\tau_\wp \psi = 2^{\frac{1}{2} v_\wp(u+\sqrt{d})}.$$

As an illustration, we suppose $v_\wp(F) \le v_\wp(E) = v_\wp(F-E) = \frac{1}{2} v_\wp(u+\sqrt{d})$, then

$$\begin{aligned}
\tau_\wp \psi &\equiv \frac{\left(\dfrac{2EF}{E^2+F^2}\right)^{v_\wp(E)-v_\wp(F)}}{\left(\dfrac{F-E}{F}\right)^{v_\wp(F)-v_\wp(E)}} \cdot 2^{v_\wp(F)} \pmod{\wp} \\
&\equiv \left(\frac{E^2+F^2}{2E(F-E)}\right)^{v_\wp(F)-v_\wp(E)} \cdot 2^{v_\wp(F)} \pmod{\wp} \\
&\equiv \left(\frac{1}{2}\right)^{v_\wp(F)-v_\wp(E)} \cdot 2^{v_\wp(F)} \pmod{\wp} \\
&\equiv 2^{\frac{1}{2} v_\wp(u+\sqrt{d})} \pmod{\wp}.
\end{aligned}$$

Since $(\alpha, Z_0) \overset{2}{=} 1, \alpha \mid y$ and $\alpha \mid b$, we do not need to consider any $\wp \mid \alpha$.

Finally, for any $\wp \mid Z_0$, we have

$$\begin{aligned}
\tau_\wp \psi &\equiv \left(\frac{E-F}{F}\right)^{2v_\wp(Z_0)} \left(-\frac{1}{2}\right)^{v_\wp(Z_0)} \pmod{\wp} \\
&\equiv \left(\frac{E^2+F^2-2EF}{-2F^2}\right)^{v_\wp(Z_0)} \pmod{\wp} \\
&\equiv \left(\frac{E}{F}\right)^{v_\wp(Z_0)} \pmod{\wp}.
\end{aligned}$$

Remark 3.11.1. With the same notations as above, we discuss more about the tame symbol of ψ. Clearly, $\left(\frac{E}{F}\right)^2 \equiv -1 \pmod{\wp}$. It follows from $\alpha^2 d + \lambda^2 = \alpha^2 u^2 - \theta^2 - 2\alpha^2 w^2 + \lambda^2 + \theta^2 \equiv 0 \pmod{Z_0}$ and $(\alpha, Z_0) \overset{2}{=} 1$ that $(\lambda, Z_0) \overset{2}{=} 1$. Suppose that $\wp \mid Z_0$ and $i \in \mathbb{Z}$ with $i^2 \equiv -1 \pmod{\wp}$. If $pO_F = \mathfrak{p}\bar{\mathfrak{p}}$, one can verify that it is impossible that both $\tau_{\mathfrak{p}}\psi = i$ and $\tau_{\bar{\mathfrak{p}}}\psi = i$ hold at the same time. This fact will be used later.

Lemma 3.12. *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free and let $\alpha \in K_2F$ with $\alpha^4 = 1$. If for any $\wp \in \Omega, \tau_\wp \alpha = \pm 1$, then $\alpha = \beta\gamma$ with $\beta^2 \in K_2O_F$ and $\gamma^2 = 1$.*

Proof. By the assumption, we see that for any $\wp \in \Omega, \tau_\wp \alpha^2 = 1$, hence, $\alpha^2 \in K_2O_F$. Since $(\alpha^2)^2 = 1$, we get $\alpha^2 = \{-1, m\}$, where $m \mid d$ or $m = n(u+\sqrt{d})$ with $n \mid d$. Let $\beta^2 = \{-1, m\}$. Then $\alpha^2 = \beta^2$. Hence, $\alpha = \beta\gamma$ with $\gamma^2 = 1$ as desired. This completes the proof.

Let $\{-1, g\} \in K_2O_F$ with $\{-1, g\} = \gamma^4$. Then for any non-dyadic place $\wp \in \Omega, (\tau_\wp \gamma)^4 \equiv 1 \pmod{\wp}$. When we consider the problem if $\{-1, g\} \in \bigtriangledown^4$, in most cases, we can choose γ with $\tau_\wp \gamma = \pm 1$. In this case, we can give a criterion for $\{-1, g\}$ to be in $\bigtriangledown^4$ or not. So we give the following

Definition 3.13. Let $\{-1, g\} \in K_2O_F$ with $\{-1, g\} = \gamma^4$. We call a case the normal case if for any non-dyadic place $\wp \in \Omega, \tau_\wp \gamma = \pm 1$.

For convenience, we introduce the following notations. For any square-free integer d and $i = 1, 3, 5, 7$, denote by d_i the product of all prime divisors of d which $\equiv i \pmod 8$. Note that $d_i = 1$ if and only if d has no prime divisor $\equiv i$ $pmod8$. So if d is odd, then $|d| = d_1 d_3 d_5 d_7$, if d is even, then $|d| = 2d_1 d_3 d_5 d_7$.

With several preparatory results, we are now in a position to give our main theorem.

Theorem 3.14. *Let d be a square-free integer and $F = \mathbb{Q}(\sqrt{d})$, and let $m \mid d$. Write $m = \pm m_1 m_3 m_5 m_7$ with $m_i \mid d_i$ for $i = 1, 3, 5, 7$. Assume there is an $\epsilon \in \{1, 2\}$ such that*

$$\epsilon m Z^2 = X^2 + dY^2 \tag{3.6}$$

is solvable, and let $X_0, Y_0, Z_0 \in \mathbb{N}$ with $(Z_0, d) = 1$ be a solution of (3.6).

(A) Suppose that $2 \notin NF$. Then $\{-1, m\} \in \bigtriangledown^4$ if and only if for $i = 1, 3, 5, 7$, there are $h_i \mid d_i$, in particular, $h_i = 1$ is permitted, and $\epsilon \in \{\pm 1, \pm 2\}$ such that for any odd prime $l \mid d$,

$$\begin{aligned}
\left(\frac{-\frac{d}{m_3 h_1 h_5}}{l}\right) &= \left(\frac{\epsilon h_3 h_7 m_5 Z_0}{l}\right), \text{if } l \mid m_3, l \nmid h_3 \text{ or } l \mid h_1 h_5, l \nmid m_5;\\
&= \left(\frac{\epsilon \frac{d}{h_3 h_7} m_5 Z_0}{l}\right), \text{if } l \mid m_3, l \mid h_3;\\
&= \left(\frac{2\epsilon h_3 h_7 \frac{d}{m_5} Z_0}{l}\right), \text{if } l \mid h_5, l \mid m_5
\end{aligned}$$

and

$$\begin{aligned}
\left(\frac{m_3 h_1 h_5}{l}\right) &= \left(\frac{\epsilon h_3 h_7 m_5 Z_0}{l}\right), \text{if } l \nmid h_1 h_3 h_5 h_7 m_3 m_5;\\
&= \left(\frac{\epsilon \frac{d}{h_3 h_7} m_5 Z_0}{l}\right), \text{if } l \mid h_3 h_7, l \nmid m_3;\\
&= \left(\frac{2\epsilon h_3 h_7 \frac{d}{m_5} Z_0}{l}\right), \text{if } l \mid m_5, l \nmid h_5.
\end{aligned}$$

(B) Suppose that $2 \in NF$.

(i) Then $\{-1, m\} \in \bigtriangledown^4$ if and only if for $i = 1, 7$, there are $h_i \mid d_i$ ($h_i = 1$ is permitted) and $\epsilon \in \{\pm 1\}$ such that for any odd prime $l \mid d$,

$$\begin{aligned}
\left(\frac{\epsilon h_1}{l}\right) &= \left(\frac{h_7 Z_0}{l}\right), \text{if } l \nmid h_1 h_7;\\
&= \left(\frac{\frac{d}{h_7} Z_0}{l}\right), \text{if } l \mid h_7
\end{aligned}$$

and

$$\left(\frac{\epsilon \frac{d}{h_1}}{l}\right) = \left(\frac{h_7 Z_0}{l}\right), \text{if } l \mid h_1$$

or

$$\begin{aligned}
\left(\frac{\epsilon h_1 (u + w)}{l}\right) &= \left(\frac{h_7 Z_0}{l}\right), \text{if } l \nmid h_1 h_7;\\
&= \left(\frac{\frac{d}{h_7} Z_0}{l}\right), \text{if } l \mid h_7
\end{aligned}$$

and

$$\left(\frac{\epsilon\dfrac{d}{h_1}(u+w)}{l}\right)=\left(\frac{h_7Z_0}{l}\right), \textit{ if } l\mid h_1.$$

(ii) Suppose that there is an $\epsilon\in\{1,2\}$ *such that*

$$\epsilon m(u+w)Z^2=X^2+dY^2 \tag{3.7}$$

is solvable and let $X_0,Y_0,Z_0\in\mathbb{N}$ *with* $(Z_0,dw)\overset{2}{=}1$ *be a solution. Then* $\{-1,m(u+\sqrt{d})\}\in\bigtriangledown^4$ *if and only if for* $i=1,7$*, there are* $h_i\mid d_i$ *(*$h_i=1$ *is permitted) and* $\epsilon\in\{\pm1\}$ *such that for any odd prime* $l\mid d$,

$$\begin{aligned}\left(\frac{\epsilon h_1}{l}\right)&=\left(\frac{h_7uZ_0}{l}\right), \textit{ if } l\nmid h_1h_7;\\ &=\left(\frac{\dfrac{d}{h_7}uZ_0}{l}\right), \textit{ if } l\mid h_7\end{aligned}$$

and

$$\left(\frac{\epsilon\dfrac{d}{h_1}}{l}\right)=\left(\frac{h_7uZ_0}{l}\right), \textit{ if } l\mid h_1,$$

or

$$\begin{aligned}\left(\frac{\epsilon h_1(u+w)}{l}\right)&=\left(\frac{h_7uZ_0}{l}\right), \textit{ if } l\nmid h_1h_7;\\ &=\left(\frac{\dfrac{d}{h_7}uZ_0}{l}\right), \textit{ if } l\mid h_7\end{aligned}$$

and

$$\left(\frac{\epsilon\dfrac{d}{h_1}(u+w)}{l}\right)=\left(\frac{h_7uZ_0}{l}\right), \textit{ if } l\mid h_1.$$

Proof. (A) We divide the proof into the following cases:

Case 1. $d\not\equiv1 \pmod 8$.

By Lemmas 3.2 and 3.10, we know that

$$\{-1,m\}=\rho^4\{m,2\}^2,$$

where $\rho\in K_2F$ with

$$\tau_\wp\rho=\begin{cases}\left(\dfrac{Y_0\sqrt{d}}{X_0}\right)^{v_\wp(Z_0)} \pmod\wp, & \text{if } \wp\mid Z_0;\\ 2 \pmod\wp, & \text{if } \wp\mid m;\\ 1 & \text{otherwise.}\end{cases}$$

By Lemmas 3.5, 3.6 and 3.7, we see that

$$\{m,2\}=\beta^4,$$

where $\beta \in K_2F$. Let $m_5 = p_1...p_j$ be the primes factorization. Then

$$\tau_\wp\beta = \begin{cases} \frac{1}{2}, & \text{if } \wp \mid m_1m_5m_7; \\ -\frac{1}{2}, & \text{if } \wp \mid m_3; \\ -1, & \text{if } \wp = \mathfrak{q}_i; \\ 1, & \text{if } \wp = \bar{\mathfrak{q}}_i (1 \le i \le j); \\ 1, & \text{otherwise.} \end{cases}$$

Here, $\mathfrak{q}_i\bar{\mathfrak{q}}_i = q_iO_F$ and q_i are primes corresponding to p_i as in Lemma 3.7. Let $q = q_1...q_j$. One can check that there is a prime $p \equiv 1 \pmod 4$ and $\epsilon_0 = 1$ or 2 such that $\epsilon_0 pZ_0H^2 = S^2 + dT^2$ is solvable. Let S_0, T_0, H_0 with $(S_0, T_0) = 1$ be a solution. And let $\xi = \left\{\frac{T_0\sqrt{d}}{S_0}, \frac{S_0^2 + dT_0^2}{S_0^2}\right\}\{-1, H_0\}$. It is immediate to verify that $\xi^4 = 1$ and

$$\tau_\wp\xi = \begin{cases} \left(\frac{T_0\sqrt{d}}{S_0}\right)^{v_\wp(Z_0)}, & \text{if } \wp \mid Z_0; \\ \frac{T_0\sqrt{d}}{S_0}, & \text{if } \wp \mid p; \\ 1, & \text{otherwise.} \end{cases}$$

Since $p \equiv 1 \pmod 4$, $p = a^2 + b^2$, where $a, b \in \mathbb{Z}$. Note that for any $\wp \mid Z_0$, $\left(\frac{T_0\sqrt{d}}{S_0}\right)^2 \equiv -1 \pmod{\wp}$, and for $\wp \mid p$, $\left(\frac{T_0\sqrt{d}}{S_0}\right)^2 \equiv -1 \pmod{\wp}$, $\left(\frac{a}{b}\right)^2 \equiv -1 \pmod{\wp}$. Let $\eta = \left\{\frac{a}{b}, \frac{p}{b^2}\right\}$ and let $\gamma = \rho\beta\xi^{-1}\eta$. Then $\gamma^4 = \{-1, m\}$. We may assume that

$$\tau_\wp\gamma = \begin{cases} -1, & \text{if } \wp = \mathfrak{p}; \\ 1, & \text{if } \wp = \bar{\mathfrak{p}} (\mathfrak{p}\bar{\mathfrak{p}} = pO_F); \\ 1, & \text{otherwise.} \end{cases}$$

Now put the above result and Lemma 3.12 together, we see that $\{-1, m\} \in \bigtriangledown^4$ if and only if for $i = 1, 3, 5, 7$ there are $h_i \mid d_i$ and $\epsilon_1 \in S(d)$ such that

$$\epsilon_1 pqm_3rZ^2 = X^2 - dY^2 \tag{3.8}$$

is solvable, where $r \equiv 1 \pmod 4$ is a prime such that

$$\epsilon_2 h_1h_3h_5h_7rZ^2 = X^2 + dY^2 \tag{3.9}$$

is solvable for some $\epsilon_2 \in S(-d)$.

But (3.8) can be rewritten as $\epsilon_1 pqrZ^2 = m_3X^2 - \frac{d}{m_3}Y^2$. Since for any odd prime $l \mid d$,

$$\left(\frac{\epsilon_2 r}{l}\right) = \begin{cases} \left(\frac{h_1h_3h_5h_7}{l}\right), & \text{if } l \nmid h_1h_3h_5h_7; \\ \left(\frac{\frac{d}{h_1h_3h_5h_7}}{l}\right) & \text{if } l \mid h_1h_3h_5h_7, \end{cases}$$

and $\left(\frac{p}{l}\right) = \left(\frac{\epsilon_0 Z_0}{l}\right)$, it is no problem now to check that (3.8) is solvable if and only if the conditions in (A) hold.

Case 2. $d \equiv 1 \pmod 8$.

One can easily see that the above method works also for the case $d < 0$ ($d \equiv 1 \pmod 8$), since there is a prime q with $\left(\frac{d}{p}\right) = 1$ such that $\epsilon_0 q m_5 Z^2 = X^2 - 2dY^2$ ($\epsilon_0 = 1$ or -2) is solvable and there is a prime $r\ equiv 1 \pmod 8$ such that $\epsilon_1 Z_0 r Z^2 = X^2 + dY^2$ is solvable for $\epsilon_1 = 1$ or -1.

So we assume $d \equiv 1 \pmod 8$ with $d > 0$ below. There are six possibilities altogether. We need to consider the cases one by one.

($\mathbb{P}1$) $m_5 \equiv 5 \pmod 8$, $\left(\frac{Z_0}{d}\right) = -1$.

($\mathbb{P}2$) $m_5 \equiv 5 \pmod 8$, $\left(\frac{Z_0}{d}\right) = 1, d_3 d_7 \neq 1$.

($\mathbb{P}3$) $m_5 \equiv 5 \pmod 8$, $\left(\frac{Z_0}{d}\right) = 1, d_3 d_7 = 1$.

($\mathbb{P}4$) $m_5 \equiv 1 \pmod 8$, $\left(\frac{Z_0}{d}\right) = 1$.

($\mathbb{P}5$) $m_5 \equiv 1 \pmod 8$, $\left(\frac{Z_0}{d}\right) = -1, d_3 d_7 \neq 1$.

($\mathbb{P}6$) $m_5 \equiv 1 \pmod 8$, $\left(\frac{Z_0}{d}\right) = -1, d_3 d_7 = 1$.

Remember that we have an element $\rho \in K_2F$ with

$$\tau_\wp \rho = \begin{cases} \left(\dfrac{Y_0\sqrt{d}}{X_0}\right)^{v_\wp(Z_0)}, & \text{if } \wp \mid Z_0; \\ 2; & \text{if } \wp \mid m; \\ 1, & \text{otherwise} \end{cases}$$

such that $\{-1, m\} = \rho^4 \{m, 2\}^2$.

If $m_5 \equiv 5 \pmod 8$, then by Lemma 3.7 we have a prime q with $\left(\frac{d}{q}\right) = -1$ such that $q m_5 Z^2 = X^2 - 2dY^2$ is solvable, hence we can find an element $\beta \in K_2F$ with

$$\tau_\wp \beta = \begin{cases} \dfrac{1}{2}, & \text{if } \wp \mid m_5; \\ i (i^2 \equiv -1 \pmod{\wp}), & \text{if } \wp = qO_F; \\ 1, & \text{otherwise}, \end{cases}$$

such that $\beta^2 = \{m_5, 2\}$.

If $m_5 \equiv 1 \pmod 8$, then also by Lemma 3.7 we have a prime q with $\left(\frac{d}{q}\right) = 1$ such that $q m_5 Z^2 = X^2 - 2dY^2$ is solvable, and we can find an element $\beta \in K_2F$ with

$$\tau_\wp \beta = \begin{cases} \dfrac{1}{2}, & \text{if } \wp \mid m_5; \\ -1, & \text{if } \wp = \mathfrak{q}; \\ 1, & \text{if } \wp = \bar{\mathfrak{q}} (\mathfrak{q}\bar{\mathfrak{q}} = qO_F); \\ 1, & \text{otherwise}, \end{cases}$$

such that $\beta^2 = \{m_5, 2\}$.

For ($\mathbb{P}1$), there is a prime $r \equiv 1 \pmod 4$ such that $rqZ_0H^2 = S^2 + dT^2$ is solvable. Let $S_0, T_0, H_0 \in \mathbb{Z}$ with $(S_0, T_0) = 1$ be a solution and let

$$\xi = \left\{\frac{T_0\sqrt{d}}{S_0}, \frac{S_0^2 + dT_0^2}{S_0^2}\right\} \{-1, H_0\} \left\{\frac{b}{a}, \frac{r}{b^2}\right\},$$

where $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = r$. We have $\xi^4 = 1$ and

$$\tau_\wp \xi = \begin{cases} \left(\dfrac{T_0\sqrt{d}}{S_0}\right)^{v_\wp(Z_0)}, & \text{if } \wp \mid Z_0; \\ \dfrac{T_0\sqrt{d}}{S_0}; & \text{if } \wp = qO_F; \\ -1, & \text{if } \wp = \mathfrak{r}; \\ 1, & \text{if } \wp = \bar{\mathfrak{r}}, \text{ where } \mathfrak{r}\bar{\mathfrak{r}} = rO_F; \\ 1, & \text{otherwise.} \end{cases}$$

It is clear that for $\wp \mid qZ_0$, $\left(\dfrac{T_0\sqrt{d}}{S_0}\right)^2 \equiv -1 \pmod{\wp}$. Hence, we can find an element $\gamma \in K_2F$ with

$$\tau_\wp \gamma = \begin{cases} -1, & \text{if } \wp = \mathfrak{r}; \\ 1, & \text{if } \wp = \bar{\mathfrak{r}} (\mathfrak{r}\bar{\mathfrak{r}} = rO_F; \\ 1, & \text{otherwise} \end{cases}$$

such that $\gamma^4 = \{-1, m\}$. This is the normal case and the same argument just as in the case $d \not\equiv 1$ gives the desired result.

For $(\mathbb{P}2)$, there is a prime $r \equiv 1 \pmod 4$ such that $rqZ_0p'H^2 = S^2 + dT^2$ is solvable, where $p' \mid d_3d_7$ is a prime. Constructing ξ as in $(\mathbb{P}1)$, one sees that the ξ has the same property. So we have returned to the similar setting. We point out that in this case, h_3h_7 in the theorem will be h_3h_7p', if we use the same notation as before. But everything remains valid, since h_3h_7 in the theorem is arbitrary.

For $(\mathbb{P}3)$, there is a prime $r \equiv 1 \pmod 4$ such that

$$rZ_0H^2 = S^2 + dT^2$$

is solvable. Then a similar process shows that there is an element $\gamma \in K_2F$ with

$$\tau_\wp \gamma = \begin{cases} i (i^2 \equiv -1 \pmod{\wp}), & \text{if } \wp = qO_F; \\ \pm 1, & \text{otherwise.} \end{cases}$$

such that $\gamma^4 = \{-1, m\}$. Hence, $\{-1, m\} \in \bigtriangledown^4$ if and only if we can find an element $\eta \in K_2F$ satisfying that for any $\wp \in \Omega$, $\tau_\wp\gamma = \tau_\wp\eta$ and $\eta^4 = 1$. By Lemma 2.8, there are $x, y \in F^*$ such that $\eta = \{x, x^2+1\}\{-1, y\}$ since $\eta^4 = 1$. Note that

$$\tau_\wp \eta^2 = \begin{cases} -1, & \text{if } \wp = qO_F; \\ 1, & \text{otherwise.} \end{cases}$$

Therefore, $\tau_\wp(\eta^2\{-1, q\}) = 1$ holds for any $\wp \in \Omega$. In other words, $\eta^2\{-1, q\} \in K_2O_F$. This implies that there is an $m \mid d$ such that $\eta^2\{-1, q\} = \{-1, m\}$. But, $\eta^2 = \{x^2, x^2+1\} = \{-1, x^2+1\}$. Hence, $\{-1, q(x^2+1)\} = \{-1, m\}$. It follows that $q(x^2+1) = mf^2$ or $2mf^2$, where $f \in F^*$. So q is the sum of two squares in F. Since $d \equiv 1 \pmod 8$, there are two dyadic places in Ω, say, $\mathfrak{q}, \bar{\mathfrak{q}}$. We have $\left(\dfrac{-1, q}{\mathfrak{q}}\right) = \left(\dfrac{-1, q}{\bar{\mathfrak{q}}}\right) = -1$, since $F_{\mathfrak{q}} \cong F_{\bar{\mathfrak{q}}} \cong \mathbb{Q}_2$. Hence, it is impossible that q is the sum of two squares in F. So, $\{-1, m\} \notin \bigtriangledown^4$.

On the other hand, one can see that the conditions in (A) read as the following in this case.

(A1) $$\left(\dfrac{\dfrac{d}{h_1h_5}}{l}\right) = \left(\dfrac{\epsilon m_5 Z_0}{l}\right), \qquad \text{if } l \mid h_1h_5, l \nmid m_5.$$

(A2) $$\left(\frac{\frac{d}{h_1h_5}}{l}\right) = \left(\frac{2\epsilon\frac{d}{m_5}Z_0}{l}\right), \qquad \text{if } l \mid h_5, l \mid m_5.$$

(A3) $$\left(\frac{h_1h_5}{l}\right) = \left(\frac{\epsilon m_5 Z_0}{l}\right), \qquad \text{if } l \nmid h_1h_5, l \nmid m_5.$$

(A4) $$\left(\frac{h_1h_5}{l}\right) = \left(\frac{2\epsilon\frac{d}{m_5}Z_0}{l}\right), \qquad \text{if } l \nmid h_5, l \mid m_5.$$

Let $m_5 = T_1T_2$ and $\frac{d}{m_5} = S_1S_2$, where $T_1 = (m_5, h_5), T_2 = \frac{m_5}{T_1}, S_1 = (\frac{d}{m_5}, h_1h_5)$ and $S_2 = \frac{d}{m_5S_1}$.

We get from $A1, A2, A3$ and $A4$ the following

(B1) $$\left(\frac{\frac{d}{h_1h_5}}{S_1}\right) = \left(\frac{\epsilon m_5 Z_0}{S_1}\right).$$

(B2) $$\left(\frac{\frac{d}{h_1h_5}}{T_1}\right) = \left(\frac{2\epsilon\frac{d}{m_5}Z_0}{T_1}\right).$$

(B3) $$\left(\frac{h_1h_5}{S_2}\right) = \left(\frac{\epsilon m_5 Z_0}{S_2}\right).$$

(B4) $$\left(\frac{h_1h_5}{T_2}\right) = \left(\frac{2\epsilon\frac{d}{m_5}Z_0}{T_2}\right).$$

respectively.

Putting the four identities together and using $S_1T_1 = h_1h_5$ and $S_2T_2 = \frac{d}{h_1h_5}$, we obtain

$$\left(\frac{h_1h_5}{\frac{d}{h_1h_5}}\right)\left(\frac{\frac{d}{h_1h_5}}{h_1h_5}\right) = \left(\frac{\epsilon Z_0}{d}\right)\left(\frac{2\frac{d}{m_5}}{m_5}\right)\left(\frac{m_5}{\frac{d}{m_5}}\right).$$

Clearly, the left hand side is 1. But the right-hand side is -1, since $d \equiv 1 \pmod 8$, $\left(\frac{\epsilon Z_0}{d}\right) = 1$ and $\left(\frac{2}{m_5}\right) = -1$. This gives the desired result.

Clearly, $(\mathbb{P}4)$ is the same as the case $d \not\equiv 1 \pmod 8$.

$(\mathbb{P}5)$ is the same as $(\mathbb{P}2)$. In fact, there is a prime $r \equiv 1 \pmod 4$ such that $rqZ_0p'Z^2 = X^2 + dY^2$ is solvable, the rest is the same as before.

$(\mathbb{P}6)$ is the same as $(\mathbb{P}3)$. More precisely, in this case, $\{-1, m\} \notin \nabla^4$ (but there is $\gamma \in K_F$ such that $\gamma^4 = \{-1, m\}$) and at least one of the conditions in (A) fails to be true.

(B) $2 \in NF$.

We mention that if $d = u^2 - 2w^2$, then the fact $\beta^4 = 1$ with $\beta^2 \in K_2O_F$ will imply that $\beta^2 = \{-1, m\}$ with $m \mid d$ or $\beta^2 = \{-1, n(u+\sqrt{d})\}$ with $n \mid d$. We have dealt with the case where $\beta^2 = \{-1, m\}$. If $\beta^2 = \{-1, n(u+\sqrt{d})\}$, then using Lemma 3.12, we see that there is an $\alpha \in K_2O_F$ with $\alpha^2 = \beta^2$ and

$$\tau_\wp \alpha = \begin{cases} -1, & \text{if } \wp = \mathfrak{p}; \\ 1, & \text{if } \wp = \bar{\mathfrak{p}} (\mathfrak{p}\bar{\mathfrak{p}} = pO_F); \\ 1, & \text{otherwise,} \end{cases}$$

where $p \equiv 1 \pmod 4$ with $\left(\dfrac{d}{p}\right) = 1$ being a prime such that $pn(u+w)Z^2 = X^2 + dY^2$ is solvable.

It is obvious that $d_3 = d_5 = 1$, since $2 \in NF$. Let $m \mid d$ with $m > 0$. Then we always have $\{m, 2\} = \beta^2$, where $\beta \in K_2F$ with

$$\tau_\wp \beta = \begin{cases} \dfrac{1}{2}, & \text{if } \wp \mid m; \\ 1, & \text{otherwise.} \end{cases}$$

We also have $\{u+\sqrt{d}, 2\} = \gamma^2$. For the tame symbol of γ, see Lemma 3.9 .

Let us see each case below.

Case 1. $d < 0$ or $d \not\equiv 1 \pmod 8$.

In this case, there is a prime $r \equiv 1 \pmod 8$ such that $\epsilon r Z_0 Z^2 = X^2 + dY^2$ is solvable for $\epsilon = 1$ or -1. On the other hand, we have $\{u+\sqrt{d}, 2\} = \gamma^2$ and for any non-dyadic place $\wp$, if $\wp \mid (u+\sqrt{d})$, then $\tau_\wp \gamma = \dfrac{1}{2}$, otherwise ± 1. Hence, the discussion in the case where $d \not\equiv 1 \pmod 8$ with $2 \notin NF$ is also valid here.

Case 2. $d > 0, d \equiv 1 \pmod 8$.

First, we consider if $\{-1, n(u+\sqrt{d}\} \in \bigtriangledown^4$.

We have six possibilities:

$(\mathbb{P}'1)$. $\left(\dfrac{Z_0}{d}\right) = \left(\dfrac{u}{d}\right) = 1$.

$(\mathbb{P}'2)$. $\left(\dfrac{Z_0}{d}\right) = \left(\dfrac{u}{d}\right) = -1$.

$(\mathbb{P}'3)$. $\left(\dfrac{Z_0}{d}\right) = 1, \left(\dfrac{u}{d}\right) = -1$, either $d_7 \neq 1$ or $\left(\dfrac{u+w}{d}\right) = -1$.

$(\mathbb{P}'4)$. $\left(\dfrac{Z_0}{d}\right) = -1, \left(\dfrac{u}{d}\right) = 1$, either $d_7 \neq 1$ or $\left(\dfrac{u+w}{d}\right) = -1$.

$(\mathbb{P}'5)$. $\left(\dfrac{Z_0}{d}\right) = -1, \left(\dfrac{u}{d}\right) = 1, d_7 = 1, \left(\dfrac{u+w}{d}\right) = 1$.

$(\mathbb{P}'6)$. $\left(\dfrac{Z_0}{d}\right) = 1, \left(\dfrac{u}{d}\right) = -1, d_7 = 1, \left(\dfrac{u+w}{d}\right) = 1$.

$(\mathbb{P}'1)$ is the normal case.

For $(\mathbb{P}'2)$, there is a prime $r \equiv 1 \pmod 4$ such that $rqZ_0Z^2 = X^2 + dY^2$ is solvable, this is also the normal case.

For $(\mathbb{P}'3)$, there is a prime $r \equiv 1 \pmod 4$ such that $rqZ_0d_7Z^2 = X^2 + dY^2$ if $d_7 \neq 1$ or $rqZ_0(u+w)Z^2 = X^2 + dY^2$ if $d_7 = 1$, is solvable, the former is the normal case. For the latter, constructing E, F as was done just before L emma 3.11, we have $E^2 + F^2 = rqZ_0(u+\sqrt{d})(2\alpha Z)^2$. Let $\theta = \left\{\dfrac{E}{F}, \dfrac{E^2+F^2}{F^2}\right\}\{-1, \alpha Z\}\left\{\dfrac{a}{b}, \dfrac{r}{b^2}\right\}$, where $a, b \in \mathbb{Z}$ such that $r = a^2 + b^2$. Then $\theta^4 = 1$. We may assume that

$$\tau_\wp \theta = \begin{cases} \left(\dfrac{E}{F}\right)^{v_\wp(Z_0)}, & \text{if } \wp \mid Z_0; \\ \dfrac{E}{F}, & \text{if } \wp = qO_F; \\ -1, & \text{if } \wp = \mathfrak{r}; \\ 1, & \text{if } \wp = \bar{\mathfrak{r}}\ (\mathfrak{r}\bar{\mathfrak{r}} = rO_F); \\ 1, & \text{otherwise.} \end{cases}$$

Since $\left(\frac{E}{F}\right)^2 = -1 \pmod{qZ_0}$, we get an element $\gamma \in K_2F$ with $\tau_\wp\gamma = -1$ only for $\wp = \mathfrak{r}$, otherwise 1 such that $\gamma^4 = \{-1, n(u+\sqrt{d})\}$. This is again the normal case.

($\mathbb{P}'4$) is the same as ($\mathbb{P}'3$).

($\mathbb{P}'5$) and ($\mathbb{P}'6$) are the same as ($\mathbb{P}3$).

Finally, we study if $\{-1, n\} \in \bigtriangledown^4$. There are three cases:

($\mathbb{P}''1$). $\left(\frac{Z_0}{d}\right) = 1$.

($\mathbb{P}''2$). $\left(\frac{Z_0}{d}\right) = -1$, either $d_7 \neq 1$ or $\left(\frac{u+w}{d}\right) = -1$.

($\mathbb{P}''3$). $\left(\frac{Z_0}{d}\right) = -1, d_7 = 1, \left(\frac{u+w}{d}\right) = 1$.

Clearly, ($\mathbb{P}''1$) is the normal case. Regarding $u + \sqrt{d}$ disappears, we easily see that ($\mathbb{P}''2$) and ($\mathbb{P}''3$) are the same as ($\mathbb{P}'4$) and ($\mathbb{P}'5$) respectively.

Now, we complete the proof of our theorem.

Corollary 3.15. *Let $F = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ square-free be a real quadratic field, and let ε be the fundamental unit of F. If $N\varepsilon = -1$, then in $\mathbb{Q}(\sqrt{-d})$, $\{-1,-1\} \in \bigtriangledown^4$, hence, if the 8-rank of $K_2O_{\mathbb{Q}(\sqrt{-d})} = 0$, then $\{-1,-1\} = 1$.*

Proof. It follows from $N\varepsilon = -1$ that $X^2 - dY^2 = -4$ has a nontrivial solution in $\mathbb{Z}$, hence, we can take $Z_0 = 2$. In view of Theorem 3.14, one sees that our result follows.

Remark 3.15.1. The converse of the above corollary is also true if d is odd, more precisely, we have shown that if the 8-rank of $K_2O_{\mathbb{Q}(\sqrt{-d})} = 0$, then $\{-1,-1\} = 1$ in $K_2\mathbb{Q}(\sqrt{-d})$ if and only if $N\varepsilon = -1$. See [18] for more in details.

4. The 8-rank of K_2O_F and the Tate kernels of imaginary quadratic fields

In this section, we apply Theorem 3.14 to the imaginary quadratic fields case. We compute the 8-rank of K_2O_F in some cases. For a given number field (not totally real), it would be an interesting problem to give an explicit structure of the Tate kernel. In [16], we have done this for some imaginary quadratic fields. Here we will also deal with this problem in some new cases.

Recall that for a number field F, the Tate kernel of F is defined to be $\Delta = \{\alpha \in F^* \mid \{-1, \alpha\} = 1\}$. For an imaginary quadratic field F, we know from [20] that $[\Delta : F^{*2}] = 4$. Hence, $\Delta = F^{*2} \cup 2F^{*2} \cup \delta F^{*2} \cup 2\delta F^{*2}$. So it is enough for us to find such $\delta \in F^*$.

It is convenient for us to fix some necessary notations.

$$
\begin{aligned}
u, w: &\quad u, w \in \mathbb{Z}, u^2 - 2w^2 = d.\\
v: &\quad v = u + w.\\
r_{2^n}: &\quad 2^n\text{-rank of } K_2O_F (n \in \mathbb{N}.)\\
Z_{-1}: &\quad -{Z_{-1}}^2 = X^2 + dY^2, \text{where } X, Y, Z_{-1} \in \mathbb{N} \text{ with } (X,Y) = 1.\\
Z_v: &\quad vZ_v^2 = X^2 + dY^2, \text{where } X, Y, Z_v \in \mathbb{N} \text{ with } (X,Y) = 1.
\end{aligned}
$$

Theorem 4.1. *Let $F = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field. Then we have the following Table 1.*

Table 1

d	r_2	r_4	r_8	Tate Kernels (δ)
$-p$ ($p \equiv 1 \pmod{16}$)	1	1	1	
$-p$ ($p \equiv 9 \pmod{16}$)	1	1	0	-1
$-p$ ($p \equiv 7 \pmod 8$)	1	0	0	$u+\sqrt{d}$ with $u+w \equiv 1 \pmod 4$
$-2p$ ($p \equiv 1 \pmod{16}$)	1	1	0 if $(\frac{2}{Z_{-1}}) = -1$	$(\frac{Z_v}{p})u+\sqrt{d}$
			0 if $(\frac{2}{Z_v}) = -1, (\frac{2}{Z_{-1}}) = 1$	-1
			1 if $(\frac{2}{Z_v}) = (\frac{2}{Z_{-1}}) = 1$	
$-2p$ ($p \equiv 9 \pmod{16}$)	1	0	0	-1
$-2p$ ($p \equiv 7 \pmod 8$)	1	0	0	$(\frac{u+w}{p})u+\sqrt{d}$

Remark 4.1.1. Let p be a prime, $F = \mathbb{Q}(\sqrt{-p})$. The following result in the above Theorem

$$8-\mathrm{rank}K_2O_F = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{16}; \\ 0, & \text{if } p \equiv 9 \pmod{16} \end{cases}$$

was first conjectured by J.Hurrelbrink.

Remark 4.1.2. For the convenience of readers, we list the known results for r_2 and r_4 (see [1] and [4]). It is an easy consequence of [1] that $r_2 = 0$ for $d = -p$ or $-2p$ with $p \not\equiv \pm 1 \pmod 8$.

Proof. We know that in all our cases K_2O_F can be generated by $\{-1,-1\}$ and $\{-1, u+\sqrt{d}\}$.

If $d = -p$ or $-2p$ with $p \equiv 7 \pmod 8$, then $-Z^2 = X^2 + dY^2$ is not solvable in $\mathbb{Z}$, hence, $\{-1,-1\} \notin \nabla^2$, so $r_4 = 0$.

If $d = -p$ or $-2p$ with $p \equiv 1 \pmod 8$, then we have $X, Y, Z_{-1} \in \mathbb{Z}$ with $(X,Y) = 1$ and

$$X^2 + dY^2 = -{Z_{-1}}^2. \tag{4.1}$$

Let us investigate the two cases individually below.

The case $d = -p, p \equiv 1 \pmod{16}$. It follows from $-p = u^2 - 2w^2$ that $-p = (u+w)(u-w) - w^2$. Hence, we have $\left(\dfrac{v}{p}\right) = 1$. So $X^2 - pY^2 = vZ_v^2$ is solvable, and we let $X, Y, Z_v \in \mathbb{Z}$ with $(X,Y) = 1$ be a solution. By Corollary 3.15, we have $\{-1,-1\} \in \nabla^4$. On the other hand, $-p = u^2 - 2w^2$

implies that $u \equiv \pm 3 \pmod 8$ if $p \equiv 9 \pmod{16}$ and $u \equiv \pm 1 \pmod 8$ if $p \equiv 1 \pmod{16}$. Also from $-p = u^2 - 2w^2$, we see that $\left(\frac{u}{p}\right) = \left(\frac{2}{|u|}\right)$. Hence, $\left(\frac{u}{p}\right) = -1$ if $p \equiv 9 \pmod{16}$ and $\left(\frac{u}{p}\right) = 1$ if $p \equiv 1 \pmod{16}$. Note that we always have $\left(\frac{v}{p}\right) = \left(\frac{Z_v}{p}\right) = 1$. So we obtain from Theorem 3.14 the desired result for this case.

The case $d = -2p, p \equiv 1 \pmod 8$. It is clear that $\{-1,-1\} \in \nabla^2$. It follows from $-2p = u^2 - 2w^2$ that $2 \mid u$. We have $p \equiv 1 \pmod{16}$ if and only if $\left(\frac{2}{|u+w|}\right) = 1$, equivalently, $\{-1, u+\sqrt{d}\} \in \nabla^2$ and $p \equiv 9 \pmod{16}$ if and only if $\left(\frac{2}{|u+w|}\right) = -1$, equivalently, $\{-1, u+\sqrt{d}\} \notin \nabla^2$. Let $|u| = 2u'$. Then $-p = 2u'^2 - w^2$. So, $\left(\frac{p}{u'}\right) = 1$. Furthermore, $\left(\frac{u'}{p}\right) = \left(\frac{2u'}{p}\right) = 1$. If $\left(\frac{2}{|v|}\right) = -1$, then $vZ^2 = X^2 - 2pY^2$ has no nontrivial solution in $\mathbb{Z}$. Hence, $\{-1, u+\sqrt{d}\} \notin \nabla^4$. If $\left(\frac{2}{|v|}\right) = 1$, then $vZ_v^2 = X^2 - 2pY^2$ is solvable in $\mathbb{Z}$. Hence, if $\left(\frac{2}{Z_v}\right) = \left(\frac{2}{Z_{-1}}\right) = 1$, then $\{-1,-1\} \in \nabla^4$ and $\{-1, u+\sqrt{d}\} \in \nabla^4$; if $\left(\frac{2}{Z_v}\right) = 1, \left(\frac{2}{Z_{-1}}\right) = -1$, then $\{-1,-1\} \notin \nabla^4$ but $\{-1, u+\sqrt{d}\} \in \nabla^4$, thus $u+\sqrt{d}$ is in the Tate kernel; if $\left(\frac{2}{Z_v}\right) = -1, \left(\frac{2}{Z_{-1}}\right) = 1$, then $\{-1,-1\} \in \nabla^4$ but $\{-1, u+\sqrt{d}\} \notin \nabla^4$, thus -1 is in the Tate kernel; if $\left(\frac{2}{Z_v}\right) = \left(\frac{2}{Z_{-1}}\right) = -1$, then $\{-1,-1\}, \{-1, u+\sqrt{d}\} \notin \nabla^4$ but $\{-1, -u-\sqrt{d}\} \in \nabla^4$, thus $-u-\sqrt{d}$ is in the Tate kernel.

This completes the proof.

5. The 2-Sylow subgroups of K_2O_F for real quadratic fields

Theorem 5.1. *With the same notations as in section 4. Let $F = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. Assume $u > 0$. Then we have the following Table 2.*

Table 2

<table>
<tr><th>d</th><th>r_2</th><th>r_4</th><th>r_8</th><th>r_{16}</th></tr>
<tr><td rowspan="3">$p\ (p \equiv 1 \pmod 8)$</td><td rowspan="3">3</td><td rowspan="2">1
if $u+w \equiv 1 \pmod 4$</td><td>1
if $(\frac{-2}{u}) = (\frac{-1}{Z_v})$</td><td></td></tr>
<tr><td>0
otherwise</td><td>0</td></tr>
<tr><td>0
otherwise</td><td>0</td><td>0</td></tr>
<tr><td>$p\ (p \equiv 7 \pmod{16})^*$</td><td>2</td><td>1</td><td>1</td><td>0</td></tr>
<tr><td>$p\ (p \equiv 15 \pmod{16})$</td><td>2</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td rowspan="3">$2p\ (p \equiv 1 \pmod 8)$</td><td rowspan="3">3</td><td rowspan="2">1
if $(\frac{-2}{u+w}) = 1$</td><td>1
if $(\frac{-2}{Z_v}) = (\frac{-1}{u'})\ (u' = \frac{u}{2})$</td><td></td></tr>
<tr><td>0
otherwise</td><td>0</td></tr>
<tr><td>0
otherwise</td><td>0</td><td>0</td></tr>
<tr><td rowspan="3">$2p\ (p \equiv 7 \pmod 8)$</td><td rowspan="3">2</td><td rowspan="2">1
if $(\frac{2}{u+w}) = 1$</td><td rowspan="2">1</td><td>1
if $(\frac{2}{Z_v}) = 1$</td></tr>
<tr><td>0
otherwise</td></tr>
<tr><td>1
otherwise</td><td>0</td><td>0</td></tr>
</table>

Remark 5.1.1. The results for r_2 and r_4 are known. In particular, $r_2 = 2$ and $r_4 = 0$ if $d = p$ or $2p$ with $p \not\equiv \pm 1 \pmod 8$. For (*), see also [3], [22].

Proof. Clearly, $\{-1,-1\}, \{-1, u_i + \sqrt{d}\}$ generate ${}_2K_2O_F$, where $u_i^2 - d = c_i w_i^2$, $u_i, w_i, c_i \in \mathbb{Z}$ and

$c_i \in NF \cap \{-1, 2, -2\}$. Of course, we only need to consider whether $u + \sqrt{d} \in \bigtriangledown^2$ or $\bigtriangledown^4$, where $u^2 - d^2 = 2w^2$.

The case $d = p \equiv 1 \pmod 8$.

If $\left(\frac{v}{p}\right) = -1$, equivalently, $v \equiv 3 \pmod 4 (v > 0)$, then $\{-1, u + \sqrt{d}\} \notin \bigtriangledown^2$, hence, $r_4 = 0$.

Suppose that $\left(\frac{v}{p}\right) = 1$. If $\left(\frac{-2}{u}\right) = \left(\frac{-1}{Z_v}\right)$, then $\left(\frac{u}{p}\right) = \left(\frac{Z_v}{p}\right)$, hence, $\{-1, u + \sqrt{d}\} \in \bigtriangledown^4$, so $r_8 = 1$, otherwise, $\{-1, u + \sqrt{d}\} \notin \bigtriangledown^4$, hence, $r_8 = 0$.

The case $d = p \equiv 7 \pmod 8$.

It is obvious that $vZ_v^2 = X^2 + pY^2$ is solvable. Moreover, we have $\left(\frac{Z_v}{p}\right) = 1$. It follows from $p = u^2 - 2w^2$ that $\left(\frac{p}{u}\right) = \left(\frac{-2}{u}\right)$. Hence, if $p \equiv 7 \pmod{16}$ then $u \equiv \pm 3 \pmod 8$, hence, $\left(\frac{u}{p}\right) = -1$, taking $\epsilon = -1$, we obtain from Theorem 3.14 that $r_8 = 1$ and $r_{16} = 0$ since $\epsilon < 0$. If $p \equiv 15 \pmod{16}$, then $u \equiv \pm 1 \pmod 8$, hence, $\left(\frac{u}{p}\right) = 1$, taking $\epsilon = 1$, we see that $r_8 = 1$ and $r_{16} = 1$ since $\epsilon > 0$.

The case $d = 2p, p \equiv 1 \pmod 8$.

If $\left(\frac{-2}{v}\right) = -1$, then $\left(\frac{v}{p}\right) = -1$, hence, $\{-1, u + \sqrt{d}\} \notin \bigtriangledown^2$, so $r_4 = 0$.

Suppose $\left(\frac{-2}{v}\right) = 1$. If $\left(\frac{-1}{u'}\right) = \left(\frac{-2}{Z_v}\right)$ $(u' = \frac{1}{2}u)$, then $\left(\frac{u}{p}\right) = \left(\frac{Z_v}{p}\right)$, hence, $\{-1, u + \sqrt{d}\} \in \bigtriangledown^4$, hence, $r_8 = 1$, otherwise, $r_8 = 0$.

The case $d = 2p, p \equiv 7 \pmod 8$

If $\left(\frac{2}{v}\right) = 1$, then $v \equiv \pm 1 \pmod 8$, hence, $\left(\frac{v}{p}\right) = 1$, since $\left(\frac{-2p}{v}\right) = 1$. On the other hand, we have $\left(\frac{u}{p}\right) = 1$. One can verify that $\left(\frac{Z_v}{p}\right) = \left(\frac{2}{Z_v}\right)$. Hence, if $\left(\frac{2}{Z_v}\right) = 1$, taking $\epsilon = 1$, we see at once that $r_8 = r_{16} = 1$; if $\left(\frac{2}{Z_v}\right) = -1$, taking $\epsilon = -1$, we get $r_8 = 1$ and $r_{16} = 0$.

This proves the theorem.

Acknowledgments

The author would like to thank the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy, for hospitality, where this work was done. He is also grateful to Professors J.Browkin, J.Hurrelbrink, F.Keune, M.Kolster and A.O.Kuku for their valuable help.

References

1. J.Browkin and A.Schinzel, *On 2-Sylow subgroups of K_2O_F for quadratic fields*, J. Reine Angew. Math. **331** (1982), 104-113.
2. J.Browkin and H.Gangl, *Table of tame and wild kernels of quadratic imaginary number fields of discriminants > -5000 (conjectural values)*, Math. Computations (1998).
3. A.Candiotti and K.Kramer, *On the 2-Sylow subgroup of Hilbert kernel of K_2 of number fields*, Acta Arith. **52** (1989), 49-65.
4. P.E.Conner and J. Hurrelbrink, *The 4-rank of $K_2(o)$*, Can. J. Math. **41** (1989), 932-960.
5. P.E.Conner and J. Hurrelbrink, *On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields*, Acta Arith. **73** (1995), 59-65.
6. F.Keune, *On the structure of the K_2 of the ring of integers in a number field*, K-theory **2** (1989), 625-645.
7. J.Hurrelbrink and M.Kolster, *Tame kernels under relative quadratic extensions and Hilbert symbol*, preprint.
8. K.Ireland and M.Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York (1982).
9. M.Kolster, *The structure of the 2-Sylow subgroup of $K_2(O)$ I*, Comment. Math. Helvetic **61** (1986), 376-388.
10. B.Mazur and A.Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. **76** (1984), 179-330.
11. L.J.Mordell, *Diophantine Equations*, Academic Press, London, New York (1969).
12. J.Neukirch, *Class Field Theory*, Springer, Berlin (1986).
13. O.T.O'Meara, *Introduction to Quadratic Forms*, Springer, Berlin (1963).
14. H.R.Qin, *Elements of finite order in K_2F of fields,*, Chinese Science Bulletin **39** (1994), 449-451.
15. H.R.Qin, *2-Sylow subgroups of K_2O_F for real quadratic fields F*, Science in China **37** (1994), 1302-1313.

16. H.R.Qin, *The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields*, Acta Arith. **69** (1995), 153-169.
17. H.R.Qin, *The 4-rank of K_2O_F for real quadratic fields*, Acta Arith. **72** (1995), 323-333.
18. H.R.Qin, *The K_2, Pell's equations and the class number of real quadratic fields*, to appear.
19. A.A.Suslin, *Torsion in K_2 of fields*, K-Theory **1** (1987), 5-29.
20. J.Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257-274.
21. A.Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), 493-540.
22. J.Urbanowicz, *On the 2-primary part of a conjecture of Birch and Tate*, Acta Arith. **43** (1983), 69-81.